			FISMA		Reviewed b		DENOV NA	
			2005 Scoring Methodology		Reviewed o	A	SENCY NA	ME
			Report Grading Element	FY05 Possible Points	Agency/ Report	CIO Scoring	IG Scoring	Final Scoring
			Total possible points:	100		0	0	0
Annı	ual	Te	esting	20		0	0	0
			ercentage of the agency's systems reviewed, including	20		0	0	0
			e percentage of agency systems reviewed in FY05 was:	10		0	0	0
			GH Impact Systems	6		0	0	0
			Between 90 and 100%	6				
			Between 75 and 89% Between 60 and 74%	<u>4</u> 2	-			
-			Between 45 and 59%	0.5	-			
			44% and less	0				
			derate Impact Systems	3		0	0	0
	i)		Between 90 and 100%	3				
_			Between 75 and 89% Between 60 and 74%	<u>2</u> 1				
-			Between 45 and 59%	0.5				
			44% and less	0.0	βι			
			w Impact Systems	1	A. Annual Testing	0	0	0
			Between 96 and 100%	1	ĕ			
			Between 51and 95%	0.5	<u>a</u>			
			50% and less e percentage of contractor operations or facilities reviewed	0 10	2	0	•	•
-			GH Impact Systems	6	Ā	0	0	0
			Between 90 and 100%	6	₹			•
			Between 75 and 89%	4				
			Between 60 and 74%	2				
			Between 45 and 59%	0.5				
_		e Mo	44% and less derate Impact Systems	<u>0</u> 3		0	0	0
	ii)		Between 90 and 100%	3	_		U	U
\neg	,		Between 75 and 89%	2	_			
			Between 60 and 74%	1				
			Between 45 and 59%	0.5				
_			44% and less	0		_	•	•
			w Impact Systems Between 96 and 100%	<u>1</u>		0	0	0
			Between 51 and 100 % Between 51 and 95%	0.5				
			50% and less	0				
			e agency performs oversight and evaluation to ensure 3 Evaluation	0		FALSE	FALSE	FALSE
j	iii)	а	Between 96 and 100% (no points deducted from A1)	0%				
		b	Between 51and 95% (50% of points deducted)	-50%				
		С	50% and less (100% of points deducted)	-100%				
Plan	of	Ac	tion and Milestones (POA&M)	15		0	0	0
2 l	Has		e agency developed, implemented, and managing an	15		0	0	0
			e POA&M is an agency wide process, incorporating all	3		0	0	0
\dashv			Between 96 and 100% Between 81and 95%	<u>3</u> 2				
\dashv	i)		Between 71 and 80%	1				
二			Between 51and 70%	0.5				
二			50% and less	0	€			
			en an IT security weakness is identified, program officials	4	~~	0	0	0
\dashv			Between 96 and 100% Between 81and 95%	2	O A			
\dashv	ii)		Between 81and 95% Between 71 and 80%	1	<u>e</u>			
\neg			Between 51and 70%	0.5	es S			
		е	50% and less	0	ě			
			ogram officials, including contractors, report to the CIO on a	1	st	0	0	0
- 1	iii)		Between 96 and 100%	1	- ĕ			
— i			Between 51and 95% 50% and less	0.5 0	≥ 0			
=			D centrally tracks, maintains, and reviews POA&M activities	2	an	0	0	0
				2	uo		-	
		а	Between 96 and 100%		ctic			
	iv)	a b	Between 81and 95%	1.5	cţi			
	iv)	a b c	Between 81and 95% Between 71 and 80%	1.5 1	, Acti			
	iv)	a b c d	Between 81and 95% Between 71 and 80% Between 51and 70%	1.5 1 0.5	of Acti			
	iv)	a b c d e	Between 81and 95% Between 71 and 80% Between 51and 70% 50% and less	1.5 1 0.5 0	lan of Acti			0
i	iv)	a b c d e	Between 81and 95% Between 71 and 80% Between 51and 70%	1.5 1 0.5	B. Plan of Action and Milestones (POA&M)	0	0	0

	Г	c 1	50% and less	0				
	+		A&M process prioritizes IT security weaknesses to help	3		0	0	0
	f		Between 96 and 100%	3			Ū	
	Ţ	b I	Between 81and 95%	2				
vi)	,	c I	Between 71 and 80%	1				
	Ī		Between 51and 70%	0.5				
	Ī	е :	50% and less	0				
ertifi	_		on and Accreditation (C&A)	20		0	0	0
			percentage of systems that have been certified and	12		0	0	0
			H Impact Systems	6		0	0	0
			Between 90 and 100%	6		- i	, i	
	F		Between 75 and 89%	4				
	H		Between 60 and 74%	3	-			
	d	_	Between 45 and 59%	1	-			
			44% and less	0				
			derate Impact Systems	4		0	0	0
			Between 90 and 100%					
i)			Between 75 and 89%	2	-			
⊢ '′			Between 60 and 74%	1	-			
	t		Between 45 and 59% 44% and less	0.5				
	H			0.3				
	ŀ		/ Impact Systems	2		0	0	0
			Between 90 and 100%	2			-	
	ŀ		Between 75 and 89%	1.5				
	H	_	Between 60 and 74%	1.5				
	H		Between 45 and 59%	0.5	_			
	H		44% and less	0.5	√ €			
-	+		percentage of systems whose security controls have been	4	- ×	0	0	0
			H Impact Systems	2	٠ ا	0	0	0
	ľ		Between 90 and 100%	2	- E		U	
	H		Between 75 and 89%	1.5				
	H		Between 75 and 89% Between 60 and 74%	1.5 1	⊣ #			
	ŀ				_ ĕ			
	H		Between 45 and 59%	0.5	5			
— ii)			44% and less	0	C. Certification and Accreditation (C&A)			•
	ŀ		derate Impact Systems	1.5	2	0	0	0
	ŀ		Between 96 and 100%	1.5	ਕੂ 🗕			
			Between 51and 95%	0.5	<u> </u>			
	ŀ.		50% and less	0	⊣ <u>ĕ</u>			
	Ľ		/ Impact Systems	0.5	ဒိ	0	0	0
	L		Between 96 and 100%	0.5	⊣ 5			
			95% and less	0	į.			
			percentage of systems that have a contingency plan that	4	ပ	0	0	0
	ľ		H Impact Systems	2	ن	0	0	0
	F		Between 90 and 100%	2				
	F	_	Between 75 and 89%	1.5				
	ŀ		Between 60 and 74%	1				
	L	-	Between 45 and 59%	0.5				
— iii)) .	e '	44% and less	0				
	<u> </u>		derate Impact Systems	1.5		0	0	0
_	L	_	Between 96 and 100%	1.5				
_	L		Between 51and 95%	0.5				
_	Ļ		50% and less	0				_
_	Ľ		/ Impact Systems	0.5		0	0	0
_	L		Between 51and 100%	0.5				
	+		50% and less	0				
	1	OIG	Assessment of the Certification and Accreditation Process	0		FALSE	FALSE	FALSE
1	(OIG	C&A Evaluation					
╡	Ţ		Excellent, Good, Satisfactory (No Deduction from C&A score in					
iv))	aı	question 6i)	0%				
-	ŀ	_	Poor (-1/2 of C&A points awarded in question 6i)	-50%				
_	-	_						
	1	_	Failing (-100% of C&A Points awarded in question 6i)	10%				
onfig			tion Management	20		0	0	0
	Ţ	ls th	nere an agency wide security configuration policy?	20		0	0	0
	t	_	Yes	20				
	Ī	b I	No (Go to Section E, Question 7.i)	0				
			estions 1 through 11 only apply, if the agency has addressed the					
			Nindows XP Professional	0		0	0	0
\dashv	ŀ	-		0			_	
	Ļ	_	Between 81 and 100% or (N/A)					
	L	b I	Between 71 and 80%	-0.5				
	Г	С	70% and less or (No)	-1				
			5 /	0		0	0	0
	-	2. \	WINDOWS NI					
	-	_	Windows NT					
		a l	Between 81 and 100% or (N/A) Between 71 and 80%	0 -0.5				

	1							l
		_	70% and less or (No)	-1			_	_
		3.	Windows 2000 Professional	0		0	0	0
		а	Between 81 and 100% or (N/A)	0				
		b	Between 71 and 80%	-0.5				
		С	70% and less or (No)	-1				
			Windows 2000 Server	0	_	0	0	0
		_		0				
		-	Between 81 and 100% or (N/A)					
		-	Between 71 and 80%	-0.5	Ę			
		С	70% and less or (No)	-1	ae L			
		5.	Windows 2003 Server	0	Je J	0	0	0
		а	Between 81 and 100% or (N/A)	0	Jac			
		h	Between 71 and 80%	-0.5	<u>a</u>			
			70% and less or (No)	-1	_ ≥			
	i۱		` '		<u>.</u>			
	٠,	6. Solaris a Between 81 and 100% or (N/A)		0	ä	0	0	0
			0	_ <u>F</u>				
		b	Between 71 and 80%	-0.5	ij			
		7. I	70% and less or (No)	-1	D. Configuration Management			
			HP-UX	0		0	0	0
			Between 81 and 100% or (N/A)	0	Δ			
		_	` '					
		_	Between 71 and 80%	-0.5				
		-	70% and less or (No)	-1				
		8.	Linux	0		0	0	0
		а	Between 81 and 100% or (N/A)	0				
		b	Between 71 and 80%	-0.5				
			70% and less or (No)	-1				
		_	Cisco Router IOS	0			0	0
		_	<u> </u>	-		0	U	U
		_	Between 81 and 100% or (N/A)	0				
		b	Between 71 and 80%	-0.5				
		С	70% and less or (No)	-1				
		10.	Oracle	0		0	0	0
		а	Between 81 and 100% or (N/A)	0				
		-	Between 71 and 80%	-0.5				
		-	70% and less or (No)	-1		_	_	_
		-	Other. Specify:	0		0	0	0
		а	a Between 81 and 100% or (N/A)	0				
		b	Between 71 and 80%	-0.5				
		С	70% and less or (No)	-1				
		па	s the agency documented in its security policies special			0	0	0
	::\		Yes (No deductions)	0			•	
	")	-	,					
			No (Loss of 4 points)	-4				
	der	nt D	Detection and Response	15	and	0	0	0
5			e agency follows documented policies and procedures for	7	ē	0	0	0
	i)	а	Yes	7	lo			
		b	No	0				
			e agency ronows documented policies and procedures for	4	te	0	0	0
	iiλ		Yes	4	E. Incident Detecti Response		-	
	<i>,</i>	_		0	nt			
	_	a III	No e agency ronows defined procedures for reporting to the		de R		_	
	iii		ited States Computer Emergency Positions Team (IIS-	4	Ċ.	0	0	0
	١		Yes	4	=			
	'	b	No	0	Ш			
			•					
F. Traii	nin	a		10		0	0	0
8	па	s u i	e agency ensured security training and awareness of all	10		0	0	0
0		nlo	vees including contractors and those employees with	10 4	-	0	0	
			e percentage of agency employees (including contractors) Between 90 and 100%	4			U	0
			Between 90 and 100% Between 75 and 89%	3				
	i)			2				
			Between 60 and 74% Between 45 and 59%	1				
			44% and less	0				
			e percentage of employees with significant security	4	ng	0	0	0
			Between 90 and 100%	4	<u> </u>			•
			Between 75 and 89%	3	<u> </u>			
	ii)		Between 60 and 74%	2	F. Training			
			Between 45 and 59%	1	ш			
			44% and less	0				
		_			_			

		The agency provided the total training costs for FY05.		1			0	0	0
·	iii)	а	Yes	1					
			No	0					
		The agency explains policies regarding peer-to-peer me		1		Ī	0	0	0
	iv)		Yes	1		Ī			
		b	No	0					
G. Inv	ent	ory	(No deductions or -10 maximum)	0	0		0	0	0
9	9 What progress has the agency made to develop an inventory of			0	28		0	0	0
		Th	The agency has developed an inventory of major information	0	. 5	Ξ	0	0	0
	i)	а	Between 96 and 100%	0	Inventory ductions o	nu			
		b	95% and less (Or the agency has no inventory)	-10	ti e	maximu			
		Th	ne OIG generally agrees with the CIO on the number of	0	Ž	ma E	0	0	0
	ii)	а	Between 96 and 100%	0	G. Inventor deductions	_			
		b	95% and less	-10	0 6				
		Th	ne OIG generally agrees with the CIO on the number of	0			0	0	0
	iii)	а	Between 96 and 100%	0					
		b	95% and less	-10					
			Possible extra credit questions						
2	Do		the agency have a plan in place to fully implement the	0			0	0	0
		_	Yes						
			No						
3			ne agency begun to implement the security controls	0			0	0	0
		_	Yes						
		b	No						